

Japanese Patent Laying-Open No. 2002-344623

[0068] [A-2. Operation of First Embodiment] The operation of the present embodiment will now be described.

<1. Download Processing>

[0069] A portable telephone 50 reads and executes a program of a WWW browser from a ROM 508 when a browsing mode of a WWW page is instructed in accordance with an operational input. Then, based on HTML file data downloaded from a desired contents server 20 through the Internet 30 and a mobile communication network 40, the contents of the WWW page are displayed on a display screen. When a user instructs download of an application program to portable telephone 50 by an operational input while browsing this WWW page, download processing, which will be described below, is started.

[0070] Fig. 9 is a sequence chart illustrating the operation of contents server 20, portable telephone 50, and a UIM 60 in the case of downloading an application program from contents server 20.

[0071] As shown in the drawing, a CPU 506 of portable telephone 50 first transmits a download request to contents server 20 (step S101). This download request contains a command instructing download and information specifying an application program to be downloaded.

[0072] Upon receipt of the download request from portable telephone 50, a CPU 202 of contents server 20 reads the application program in accordance with this download request, from an AP storing region 201a (step S102). The read application program herein refers to a main body AP and a module AP paired with each other, as shown in Fig. 3. Then, CPU 202 downloads these main body AP and module AP to portable telephone 50 in a package (step S103). It is to be noted that the package to be downloaded from contents server 20 to portable telephone 50 may be subjected to compression processing or encryption processing.

[0073] Upon download of the package from contents server 20, CPU 506 of portable telephone 50 performs the following steps S104 to S107 in accordance with a JAM

shown in Fig. 8.

[0074] More specifically, CPU 506 first performs authentication processing of the downloaded package (step S104). This authentication processing is, for example, processing for checking the validity of the downloaded package by an electronic signature, or the like. After this authentication processing, CPU 506 extracts the main body AP and the module AP from the downloaded package (step S105). Then, CPU 506 transmits the module AP and a serial number (main body serial number) of portable telephone 50 read from a serial number storing region 510a, to UIM 60 (step S106). It is to be noted that data to be transmitted from portable telephone 50 to UIM 60 may be subjected to encryption processing.

[0075] CPU 506 also stores the main body AP extracted in the above-described step S106 in an AP storing region 510b in association with a serial number (module serial number) of UIM 60 currently mounted on portable telephone 50 (step S107). It is to be noted that the module serial number is transmitted to portable telephone 50 from UIM 60 when UIM 60 is mounted on portable telephone 50, and stored in a RAM 509.

[0076] Upon receipt of the module AP and the main body serial number from portable telephone 50 in the above-described step S106, a CPU 604 of UIM 60 first activates a loader in OS. Then, in accordance with this loader, CPU 604 stores the module AP in AP storing region 510b in association with the main body serial number (step S108). Thereafter, CPU 604 transmits, to portable telephone 50, an installation completion notification indicating that installation has been completed (step S109). The download processing is thereby terminated.

[0077] As described above, in the download processing, the main body AP and the module AP are downloaded collectively from contents server 20 to portable telephone 50. This can reduce a communication time period and a communication cost required for download.

[0078] <2. Access Management Processing> Fig. 10 is a sequence chart illustrating the operation of portable telephone 50 and UIM 60 in the case where portable telephone 50 makes access to subscriber information in UIM 60. This access

management processing is started when execution of the main body AP is instructed at portable telephone 50.

[0079] CPU 506 of portable telephone 50 first performs the following steps S201 to S203 in accordance with the JAM. More specifically, before executing the instructed main body AP, CPU 506 first acquires identification information (e.g., a file name) of the main body AP instructed to be executed, in order to authenticate this main body AP and the module AP corresponding thereto (step S201). The main body serial number is read from serial number storing region 510a (step S202). Then, CPU 506 transmits the acquired identification information and the main body serial number to UIM 60 (step S203).

[0080] Upon receipt of the identification information and the main body serial number from portable telephone 50, CPU 604 of UIM 60 performs the following steps S204 to S206 in accordance with a card manager in OS. More specifically, in accordance with the received identification information, CPU 604 checks whether or not the module AP corresponding to this main body AP is stored in an AP storing region 605b (step S204). A module serial number is read from a serial number storing region 605a (step S205). Then, CPU 604 transmits the result of presence/absence of storage and the module serial number to portable telephone 50 (step S206).

[0081] Upon receipt of the result of presence/absence of storage and the module serial number from UIM 60, CPU 506 of portable telephone 50 performs authentication processing of the main body AP whose program has been instructed to be executed and the module AP corresponding thereto, in accordance with the JAM (step S207).

[0082] In the present embodiment, the authentication processing of the main body AP and the module AP involves checking two points: whether the module AP corresponding to the main body AP whose program has been instructed to be executed is stored in UIM 60; and whether the current combination of portable telephone 50 and UIM 60 mounted thereon is identical to that of portable telephone 50 and UIM 60 when this main body AP and the module AP are downloaded.

[0083] For the authentication processing shown in the above-described step S207,

CPU 506 checks whether or not the module AP corresponding to the main body AP whose program has been instructed to be executed is stored in UIM 60 in accordance with the result of presence/absence of storage of the module AP transmitted from UIM 60. CPU 506 also compares the module serial number transmitted from UIM 60 with the module serial number stored in AP storing region 510b in association with the main body AP whose program has been instructed to be executed, thereby checking whether or not the combination of portable telephone 50 and UIM 60 is identical to that when this main body AP and the module AP are downloaded.

[0084] On the other hand, CPU 604 of UIM 60 also performs authentication of the main body AP and the module AP in accordance with the card manager (step S208), and the result of authentication is informed to portable telephone 50 (step S209). Herein, the authentication processing performed in step S208 is similar to that performed at portable telephone 50 side.

[0085] More specifically, CPU 604 checks whether or not the module AP corresponding to the main body AP whose program has been instructed to be executed is stored in UIM 60 in accordance with the result of presence/absence of storage of the module AP distinguished in the above-described step S204. CPU 604 also compares the main body serial number transmitted from portable telephone 50 with the module serial number stored in AP storing region 605b in association with the module AP corresponding to the main body AP whose program has been instructed to be executed, thereby checking whether or not the combination of portable telephone 50 and UIM 60 is identical to that when this main body AP and the module AP are downloaded.

[0086] Upon the authentication processing performed in this manner at both the sides of portable telephone 50 and UIM 60, CPU 506 of portable telephone 50 distinguishes whether or not mutual authentication has been established in accordance with the JAM (step S210). As a result, when mutual authentication has not been established, CPU 506 displays a message showing that authentication has not been established on the screen, and cancels execution of the main body AP (step S211). The access management processing is thereby terminated.

[0087] It is to be noted that the case in which mutual authentication has not been established specifically includes some cases such as where the module AP corresponding to the main body AP whose program has been instructed to be executed is not stored in UIM 60, and where the combination of portable telephone 50 and UIM 60 is different from the combination when this main body AP and the module AP are downloaded.

[0088] On the other hand, when it is distinguished in the above-described step S210 that mutual authentication has been established, CPU 506 first activates, on JavaVM, the main body AP whose program has been instructed to be executed to start processing of the main body AP (step S212). Then, when an access request for subscriber information in UIM 60 occurs during the processing of the main body AP (step S213), CPU 506 distinguishes whether or not this access request is permissible for ensuring security, in accordance with the JAM (step S214).

[0089] Then, when the access request is permitted, CPU 506 transmits, to UIM 60, the access request including the aforementioned access command and command pertinent information, and the identification information of the main body AP (step S215).

[0090] It is to be noted that CPU 506 advances the process into step S219 when no access request has occurred in the above-described step S213, or when the access request has been distinguished as not being permissible in the above-described step S214. Moreover, when the access request has been distinguished as not being permissible in the above-described step S214, it may be configured such that a message indicating that an access that is not permissible has occurred is displayed on the screen to stop execution of the main body AP.

[0091] Upon receipt of the access request from portable telephone 50 in the above-described step S215, CPU 604 of UIM 60 specifies a corresponding module AP in accordance with the card manager. Then, CPU 604 executes this module AP on JavaCard VM (step S216).

[0092] Then, in accordance with this module AP, CPU 604 performs access

processing including reading, rewriting, deletion, and the like of subscriber information depending on the access request from portable telephone 50 (step S216). When this access processing is terminated, CPU 604 transmits an access completion notification indicating that the access processing has been completed, to portable telephone 50 (step S218). It is to be noted that, when the access request is reading of subscriber information, the subscriber information as read is included in the access completion notification, and transmitted to portable telephone 50.

[0093] Upon receipt of the access completion notification from UIM 60, CPU 506 of portable telephone 50 distinguishes whether or not the processing of the main body AP is to be terminated (step S219), and when it is not to be terminated, CPU 506 returns the process to the above-described step S213 to continue the processing of the main body AP. When it is to be terminated, the processing of the main body AP is terminated. The access management processing is thereby terminated.

[0094] As described above, according to the the present embodiment, when execution of the main body AP acquired from contents server 20 through Internet 30 is instructed, CPU 506 of portable telephone 50 acquires a module serial number from UIM 60 mounted on portable telephone 50 for comparison with the module serial number associated with the main body AP. CPU 506 thereby distinguishes whether or not the current combination of portable telephone 50 and UIM 60 is identical to the combination of portable telephone 50 and UIM 60 when this main body AP is downloaded.

[0095] Then, when distinguished that the current combination of portable telephone 50 and UIM 60 is identical to the combination of portable telephone 50 and UIM 60 when this main body AP is downloaded, CPU 506 executes the main body AP. Then, during the processing of this main body AP, the main body AP and the corresponding module AP in UIM 60 operate cooperatively, so that access to the subscriber information stored in UIM 60 is made by portable telephone 50.

[0096] That is, execution of the main body AP is canceled and portable telephone 50 cannot make access to the subscriber information in UIM 60 in some cases, such as

where the combination of portable telephone 50 and UIM 60 during execution of the main body AP is identical to that of portable telephone 50 and UIM 60 when this main body AP is downloaded, and where the module AP corresponding to the main body AP is not stored in UIM 60.

[0097] As described, as to execution of the main body AP acquired through the Internet 30, execution is permitted only when the above-described certain conditions hold between portable telephone 50 and UIM 60, so that access to the subscriber information in UIM 60 can be made by portable telephone 50. Therefore, when executing the program acquired through the Internet 30, portable telephone 50 can make access to the subscriber information stored in UIM 60 outside portable telephone 50 in accordance with this program while ensuring security.

[0124] <First Variation> The above first embodiment has described the case in which the main body AP and the module AP are collectively downloaded from contents server 20. However, the procedure of download may be a procedure shown in Fig. 12, for example. Fig. 12 is a sequence chart showing a variation in the case of downloading an application program from contents server 20. It is to be noted that the following will mainly describe a difference from the download processing (see Fig. 9) described in the above embodiment.

[0125] As shown in the drawing, CPU 506 of portable telephone 50 first transmits a download request to contents server 20 (step S301). Upon receipt of the download request from portable telephone 50, CPU 202 of contents server 20 reads, from AP storing region 201a, a main body AP depending on this download request (step S302). Then, CPU 202 downloads the main body AP alone to portable telephone 50 (step S303).

[0126] Upon download of the main body AP from contents server 20, CPU 506 of portable telephone 50 first performs authentication processing of the downloaded main body AP in accordance with the JAM (step S304). This authentication processing is, for example, processing for checking the validity of the downloaded main body AP by an electronic signature, or the like. After this authentication processing, CPU 506

stores the main body AP in AP storing region 510b in association with the module serial number of UIM 60 mounted on portable telephone 50 (step S305). Then, CPU 506 transmits the download request for a module AP corresponding to the stored main body AP to contents server 20 (step S306).

[0127] CPU202 of contents server 20 reads, from AP storing region 201a, a module AP in accordance with the download request from portable telephone 50 (step S307). Then, CPU202 downloads the module AP to portable telephone 50 (step S308).

[0128] Upon download of the module AP from contents server 20, CPU 506 of portable telephone 50 performs authentication processing of the module AP in accordance with the JAM (step S309). Thereafter, CPU 506 transmits the module AP and the main body serial number of portable telephone 50 to UIM 60 in accordance with the JAM (step S310).

[0129] Upon receipt of the module AP and the main body serial number, CPU 604 of UIM 60 stores the module AP in AP storing region 510b in association with the main body serial number, in accordance with the loader in OS (step S311). Thereafter, an installation completion notification is transmitted to portable telephone 50 from UIM 60 (step S312), and the download processing is terminated.

[0130] As described above, the download processing may be configured to download a main body AP and a module AP separately from contents server 20.

[0131] <Second Variation> The first embodiment and the first variation have described the case in which the main body AP and the module AP are downloaded from contents server 20. However, the present invention is also applicable to the case in which the main body AP and the module AP are distributed to each portable telephone 50 from contents server 20.

[0132] In this case, contents server 20 has a distribution destination list in which communication addresses (e.g., an IP address, a mail address, etc.) of portable telephone 50 which is a distribution destination are registered. Contents server 20 distributes a main body AP and a module AP to be transmitted, to portable telephone 50 registered in the above-described distribution destination list and UIM 60 mounted

thereon.

[0133] <Third Variation> The first embodiment has described the configuration in which the main body serial number and the module serial number are used in the access management processing for performing authentication processing of the main body AP whose program has been instructed to be executed and the module AP corresponding thereto.

[0134] However, it may be configured such that, when, for example, the main body AP and the module AP are transmitted from contents server 20, identification information different for each package to be transmitted is assigned to both the main body AP and the module AP, and this identification information is used instead of the main body serial number and the module serial number.

[0135] In this case, the main body AP and the module AP as downloaded are stored in AP storing region 510b of portable telephone 50 or AP storing region 605b of UIM 60 in association with the identification information assigned by contents server 20.

Then, when performing the authentication processing of the main body AP and the module AP in the access management processing, CPU 506 of portable telephone 50 checks whether or not the identification information associated with the main body AP whose program has been instructed to be executed is identical to the identification information associated with the module AP corresponding to this main body AP.

[0136] Such a configuration enables authentication based on whether or not the main body AP and the module AP are programs downloaded in the same package. It is needless to say that the description of this variation is applicable not only to the case of download but also to the case of distribution.

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 M 3/42		H 0 4 M 3/42	E 5 B 0 1 7
G 0 6 F 1/00		G 0 6 F 12/14	3 2 0 F 5 B 0 7 6
	12/14	13/00	5 2 0 A 5 B 0 8 5
	13/00	15/00	3 3 0 C 5 K 0 1 5
	15/00		3 3 0 G 5 K 0 2 4

審査請求 未請求 請求項の数23 O L (全 22 頁) 最終頁に続く

(21) 出願番号 特願2001-142361 (P2001-142361)

(22) 出願日 平成13年5月11日 (2001.5.11)

(71) 出願人 392026893

株式会社エヌ・ティ・ティ・ドコモ

東京都千代田区永田町二丁目11番1号

(72) 発明者 ▲高▼橋 和彦

東京都千代田区永田町二丁目11番1号 株

式会社エヌ・ティ・ティ・ドコモ内

(72) 発明者 村瀬 淳

東京都千代田区永田町二丁目11番1号 株

式会社エヌ・ティ・ティ・ドコモ内

(74) 代理人 100098064

弁理士 川▲崎▼ 研二 (外1名)

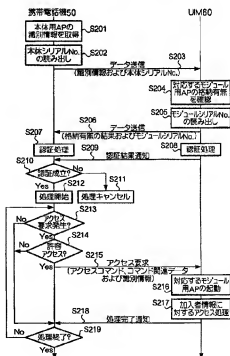
最終頁に続く

(54) 【発明の名称】 アクセス方法、通信端末、ユーザ識別モジュール、プログラムの提供方法および送信装置

(57) 【要約】

【課題】 セキュリティを確保しつつ、ネットワークを介して得たプログラムに従って当該プログラムのダウンロード元を除く当該通信端末外のリソースにアクセスできるようにすること。

【解決手段】 携帯電話機50および当該携帯電話機50に装着されたUIM60では、実行が指示された本体用APと当該本体用APに対応するモジュール用APとの相互認証が行われる。そして、両プログラムが認証された後、携帯電話機50のCPU506は、本体用APを起動し、当該本体用APの処理過程において生じたUIM60内の加入者情報に対するアクセス要求をUIM60へ出力する。UIM60のCPU604は、アクセス要求を受信すると、携帯電話機50において実行されている本体用APに対応するモジュール用APを起動し、このモジュール用APに従ってアクセス要求に応じた加入者情報の読み出しや書き込みなどを行う。



【特許請求の範囲】

【請求項1】 通信端末が電子機器に記憶されているデータにアクセスする方法であって、

前記通信端末が、ネットワークを介して取得した端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器と、前記端末用プログラムに対応した電子機器用プログラムを取得した電子機器とが同一であるか否かを判別する第1の過程と、

前記通信端末が、前記第1の過程にて同一であると判別された場合に前記端末用プログラムを実行し、当該プログラムによる処理過程において生じた前記電子機器に対するアクセス要求を当該電子機器に通知する第2の過程と、

前記電子機器が、前記通信端末において実行されている端末用プログラムに対応した電子機器用プログラムに従って、前記第2の過程にて通知されたアクセス要求に応じた処理を実行する第3の過程とを有することを特徴とするアクセス方法。

【請求項2】 前記第1の過程に先立って行われる過程であって、

前記通信端末が、ネットワークを介して端末用プログラムを取得した場合に、当該プログラムに対応した電子機器用プログラムを取得した電子機器から当該電子機器を特定する識別情報を取得して、当該識別情報を前記端末用プログラムと対応付けて記憶する第4の過程をさらに有し、

前記第1の過程では、前記通信端末が、前記端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から前記識別情報を取得して、当該識別情報と前記第4の過程にて当該端末用プログラムと対応付けて記憶された識別情報とが同一であるか否かを判別することを特徴とする請求項1記載のアクセス方法。

【請求項3】 前記第1の過程に先立って行われる過程であって、

サーバが、通信端末において実行される端末用プログラムと当該プログラムの実行に伴って電子機器において実行される電子機器用プログラムとを含むパッケージをネットワークを介して送信する場合に、前記パッケージ毎に異なる識別情報を前記端末用プログラムおよび前記電子機器用プログラムの各々に付与して送信する第5の過程と、

前記第5の過程にて送信されたパッケージのうち、前記端末用プログラムを前記通信端末が取得するとともに、前記電子機器用プログラムを前記電子機器が取得する第6の過程とをさらに有し、

前記第1の過程では、前記通信端末が、端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から当該端末用プ

ログラムに対応した電子機器用プログラムに付与されている識別情報を取得して、この識別情報と当該端末用プログラムに付与されている識別情報とが同一であるか否かを判別することとを特徴とする請求項1記載のアクセス方法。

【請求項4】 前記第2の過程は、

前記通信端末が、前記第1の過程にて同一であると判別された場合に前記端末用プログラムを実行し、当該プログラムによる処理過程において前記電子機器に対するアクセス要求が生じた場合に、許容されたアクセスの種類が規定されたアクセス規定データを参照して前記アクセス要求を許可するか否かを決定する第7の過程と、前記通信端末が前記第7の過程にて許可されたアクセス要求を前記電子機器に通知する第8の過程とを有することを特徴とする請求項1ないし3のいずれか1の請求項に記載のアクセス方法。

【請求項5】 前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであることを特徴とする請求項1ないし4のいずれか1の請求項に記載のアクセス方法。

【請求項6】 電子機器に記憶されているデータにアクセスする通信端末であって、通信端末において実行可能な端末用プログラムをネットワークを介して受信する受信手段と、

前記受信手段により受信された端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器と、前記端末用プログラムに対応した電子機器用プログラムを取得した電子機器とが同一であるか否かを判別する判別手段と、

前記判別手段により同一であると判別された場合に前記端末用プログラムを実行する実行手段とを有することを特徴とする通信端末。

【請求項7】 前記受信手段により端末用プログラムを受信した場合に、当該プログラムに対応した電子機器用プログラムを取得した電子機器から当該電子機器を特定する識別情報を取得して、当該識別情報を前記端末用プログラムと対応付けて記憶する識別情報記憶手段をさらに有し、

前記判別手段は、前記端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から前記識別情報を取得して、当該識別情報と前記識別情報記憶手段により当該端末用プログラムと対応付けて記憶された識別情報とが同一であるか否かを判別することとを特徴とする請求項6記載の通信端末。

【請求項8】 前記受信手段は、通信端末において実行可能な、識別情報が付与されている端末用プログラムをネットワークを介して受信し、

前記判別手段は、前記受信手段により受信された端末用プログラムを実行する場合に、当該プログラムの実行に

伴ってアクセスすることが定められた電子機器から当該端末用プログラムに対応した電子機器用プログラムに付与されている識別情報取得して、この識別情報と当該端末用プログラムに付与されている識別情報とが同一であるかを判断することを特徴とする請求項6記載の通信端末。

【請求項9】 前記実行手段により実行された端末用プログラムによる処理過程において生じた前記電子機器に対するアクセス要求を前記電子機器に送信する送信手段をさらに有することを特徴とする請求項6ないし8のいずれかの請求項に記載の通信端末。

【請求項10】 前記端末用プログラムに対して許可されたアクセスの種類が記憶されている許可アクセス記憶手段と、

前記実行手段により実行された端末用プログラムによる処理過程において前記電子機器に対するアクセス要求が生じた場合に、前記許可アクセス記憶手段を参照して前記アクセス要求を許可するか否かを決定する決定手段と、

前記決定手段により許可されたアクセス要求を前記電子機器に送信する送信手段とをさらに有することを特徴とする請求項6ないし8のいずれかの請求項に記載の通信端末。

【請求項11】 電子機器に記憶されているデータにアクセスする通信端末であって、当該通信端末において実行される端末用プログラムとこのプログラムの実行に伴って当該通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとをネットワークを介して受信する受信手段と、前記受信手段により受信された端末用プログラムを当該通信端末のメモリに記憶する記憶手段と、前記受信手段により受信された電子機器用プログラムを前記電子機器に送信する送信手段とを有することを特徴とする通信端末。

【請求項12】 前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであることを特徴とする請求項6ないし11のいずれかの請求項に記載の通信端末。

【請求項13】 通信端末に対して着脱自在であり、ユーザ情報が記憶されているユーザ識別モジュールであって、

当該ユーザ識別モジュールが装着された通信端末から前記ユーザ情報に対するアクセス要求を受信する受信手段と、

前記通信端末において実行されている端末用プログラムに対応したモジュール用プログラムに従って、前記受信手段により受信されたアクセス要求に応じた前記ユーザ情報に対するアクセス処理を実行する実行手段とを有することを特徴とするユーザ識別モジュール。

【請求項14】 前記通信端末からの要求に応じて、当

該ユーザ識別モジュールを特定する識別情報を前記通信端末に出力する出力手段をさらに有することを特徴とする請求項13に記載のユーザ識別モジュール。

【請求項15】 前記通信端末からの要求に応じて、前記通信端末において実行されている端末用プログラムに対応付けられたモジュール用プログラムを特定する特定手段と、

前記特定手段により特定されたモジュール用プログラムに付与されている識別情報を前記通信端末に出力する出力手段とをさらに有することを特徴とする請求項13に記載のユーザ識別モジュール。

【請求項16】 通信端末に対して着脱自在であり、ユーザ情報が記憶されているユーザ識別モジュールであって、

当該ユーザ識別モジュールが装着された通信端末から当該通信端末を特定する識別情報と当該ユーザ識別モジュールにおいて実行可能なモジュール用プログラムとを受信し、前記識別情報と前記モジュール用プログラムとを対応付けて記憶する記憶手段と、

当該ユーザ識別モジュールが装着された通信端末から前記識別情報を受信する受信手段と、

前記受信手段により受信された識別情報と前記記憶手段により記憶された識別情報とが同一であるかを判断する判断手段と、前記判断手段による判断結果を前記通信端末に出力する出力手段とを有することを特徴とするユーザ識別モジュール。

【請求項17】 サーバが、通信端末において実行される端末用プログラムと、当該プログラムの実行に伴って前記通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとをネットワークを介して通信端末に送信する第1の過程と、

前記通信端末が、前記第1の過程にて送信された端末用プログラムと電子機器用プログラムとを受信し、前記端末用プログラムを当該通信端末のメモリに記憶する第2の過程と、

前記通信端末が、前記第2の過程にて受信された電子機器用プログラムを前記電子機器に送信する第3の過程と、

前記電子機器が、前記第3の過程にて送信された電子機器用プログラムを受信し、当該電子機器用プログラムを当該電子機器のメモリに記憶する第4の過程とを有することを特徴とするプログラムの提供方法。

【請求項18】 前記第2の過程は、

前記通信端末が、前記第1の過程にて送信された端末用プログラムと電子機器用プログラムとを受信する第5の過程と、

前記通信端末が、前記電子機器から当該電子機器を特定する識別情報を取得して、当該識別情報と前記第5の過程にて受信された端末用プログラムとを対応付けて当該

通信端末のメモリに記憶する第6の過程とを有することを特徴とする請求項1記載のプログラムの提供方法。

【請求項19】 前記第1の過程では、前記サーバが、通信端末において実行される端末用プログラムと、当該プログラムの実行に伴って前記通信端末によりアクセスされる電子機器において実行される電子機器用プログラムを含むパッケージをネットワークを介して送信する場合に、前記パッケージ毎に異なる識別情報を前記端末用プログラムおよび前記電子機器用プログラムの各々に付与して送信し、

前記第2の過程では、前記通信端末が、前記第1の過程にて送信されたパッケージを受信し、当該パッケージに含まれる端末用プログラムを当該プログラムに対して付与された識別情報とともに当該通信端末のメモリに記憶し、

前記第4の過程では、前記電子機器が、前記第3の過程にて送信された電子機器用プログラムを受信し、この電子機器用プログラムを当該プログラムに対して付与された識別情報とともに当該電子機器のメモリに記憶することを特徴とする請求項1記載のプログラムの提供方法。

【請求項20】 前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであることを特徴とする請求項17ないし19のいずれか1の請求項に記載のプログラムの提供方法。

【請求項21】 通信端末において実行される端末用プログラムと、当該プログラムの実行に伴って前記通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとが記憶されている記憶手段と、通信端末からの指示に応じて、前記記憶手段から読み出した端末用プログラムと電子機器用プログラムとをネットワークを介して前記通信端末に送信する送信手段とを有することを特徴とする送信装置。

【請求項22】 前記送信手段が前記端末用プログラムと前記電子機器用プログラムとを含んだパッケージを送信する場合に、前記パッケージ毎に異なる識別情報を前記端末用プログラムおよび前記電子機器用プログラムの各々に付与する識別情報付与手段をさらに有することを特徴とする請求項21に記載の送信装置。

【請求項23】 前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであることを特徴とする請求項21または22に記載の送信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、通信端末が当該通信端末のリソースにアクセスするために好適なアクセス方法、通信端末、ユーザ識別モジュール、プログラムの提供方法および送信装置に関する。

【0002】

【従来の技術】パーソナルコンピュータやPDA(Personal Digital Assistant)などの通信端末は、ネットワークに接続されているコンピュータからプログラムをダウンロードし、このプログラムを実行することにより様々な機能を実現することができる。例えば、Java(登録商標)プログラミング言語で記述されたJavaアプレットは、ネットワークを介して通信端末にダウンロードされ、通信端末に組み込まれたブラウザ上で実行されるプログラムである。

【0003】ところで、インターネットのようなオープンネットワークを利用したデータ通信では、データの改竄、なりすましなどの危険性がある。したがって、このようなオープンネットワークを介して通信端末に提供されたプログラムのセキュリティに関する信頼性を完全に保証することは事実上困難である。

【0004】以上のようなことから、ネットワークを介して取得したプログラムの実行に関しては、例えば、Javaアプレットの場合、ダウンロードされた通信端末内のごく限られたデータおよびダウンロード元のコンピュータにしかアクセスできないように通信端末においてアクセス制限がなされている。このように、Javaアプレットの実行に際して通信端末は、ダウンロード元のコンピュータ以外の、当該通信端末に接続された周辺機器やネットワークを介して当該通信端末とデータ通信を行うことが可能な他のコンピュータなどにアクセスすることができなかった。

【0005】

【発明が解決しようとする課題】このようなアクセス制限の仕組みは、セキュリティを確保する上で一定の効果を奏するものの、ネットワークを介して提供されるプログラムに対して様々な動作制限を課することとなる。すなわち、上記アクセス制限の仕組みは、ネットワークを介して提供されたプログラムにより通信端末における機能の変更や追加などを自由に行えるという本来の利便性を損なう要因であった。

【0006】一方、ネットワークを介して得たプログラムの実行に際し、何らかのアクセス制限を設けない場合、前述したデータの改竄、なりすましなどによって、例えば、悪意の第三者により改竄されたプログラムが通信端末にダウンロードされ、当該プログラムの実行に伴う不正なアクセスによる被害が当該通信端末のみならず、他のコンピュータにまで及ぶおそれがあった。

【0007】本発明は、以上説明した事情に鑑みてなされたものであり、セキュリティを確保しつつ、ネットワークを介して得たプログラムに従って当該プログラムのダウンロード元を除く当該通信端末外のリソースにアクセスすることのできるアクセス方法、通信端末、ユーザ識別モジュール、プログラムの提供方法および送信装置を提供することを目的としている。

【0008】

【課題を解決するための手段】上記課題を解決するために、この発明は、通信端末が電子機器に記憶されているデータにアクセスする方法であって、前記通信端末が、ネットワークを介して取得した端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器と、前記端末用プログラムに対応した電子機器用プログラムを取得した電子機器とが同一であるかを判別する第1の過程と、前記通信端末が、前記第1の過程にて同一であると判別された場合に前記端末用プログラムを実行し、当該プログラムによる処理過程において生じた前記電子機器に対するアクセス要求を当該電子機器に通知する第2の過程と、前記電子機器が、前記通信端末において実行されている端末用プログラムに対応した電子機器用プログラムに従って、前記第2の過程にて通知されたアクセス要求に応じた処理を実行する第3の過程とを有するアクセス方法を提供する。

【0009】また、上記アクセス方法において、前記第1の過程に先立って行われる過程であって、前記通信端末が、ネットワークを介して端末用プログラムを取得した場合に、当該プログラムに対応した電子機器用プログラムを取得した電子機器から当該電子機器を特定する識別情報を取得して、当該識別情報を前記端末用プログラムと対応付けて記憶する第4の過程をさらに有し、前記第1の過程では、前記通信端末が、前記端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から前記識別情報を取得して、当該識別情報と前記第4の過程にて当該端末用プログラムと対応付けて記憶された識別情報とが同一であるかを判別するようにしてもよい。

【0010】また、上記アクセス方法において、前記第1の過程に先立って行われる過程であって、サーバが、通信端末において実行される端末用プログラムと当該プログラムの実行に伴って電子機器において実行される電子機器用プログラムとを含むパッケージをネットワークを介して送信する場合に、前記パッケージ毎に異なる識別情報を前記端末用プログラムおよび前記電子機器用プログラムの各々に付与して送信する第5の過程と、前記第5の過程にて送信されたパッケージのうち、前記端末用プログラムを前記通信端末が取得するとともに、前記電子機器用プログラムを前記電子機器が取得する第6の過程とをさらに有し、前記第1の過程では、前記通信端末が、端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から当該端末用プログラムに対応した電子機器用プログラムに付与されている識別情報を取得して、この識別情報と当該端末用プログラムに付与されている識別情報とが同一であるかを判別するようにしてもよい。

【0011】さらに、上記アクセス方法において、前記第2の過程は、前記通信端末が、前記第1の過程にて同

一であると判別された場合に前記端末用プログラムを実行し、当該プログラムによる処理過程において前記電子機器に対するアクセス要求が生じた場合に、許可されたアクセスの種類が規定されたアクセス規定データを参照して前記アクセス要求を許可するか否かを決定する第7の過程と、前記通信端末が前記第7の過程にて許可されたアクセス要求を前記電子機器に通知する第8の過程とを有するようにしてもよい。

【0012】また、上記アクセス方法において、前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであってもよい。

【0013】また、上記課題を解決するために、この発明は、電子機器に記憶されているデータにアクセスする通信端末であって、通信端末において実行可能な端末用プログラムをネットワークを介して受信する受信手段と、前記受信手段により受信された端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器と、前記端末用プログラムに対応した電子機器用プログラムを取得した電子機器とが同一であるかを判別する判別手段と、前記判別手段により同一であると判別された場合に前記端末用プログラムを実行する実行手段とを有する通信端末を提供する。

【0014】また、上記通信端末において、前記受信手段により端末用プログラムを受信した場合に、当該プログラムに対応した電子機器用プログラムを取得した電子機器から当該電子機器を特定する識別情報を取得して、当該識別情報を前記端末用プログラムと対応付けて記憶する識別情報記憶手段をさらに有し、前記判別手段は、前記端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から前記識別情報を取得して、当該識別情報と前記識別情報記憶手段により当該端末用プログラムと対応付けて記憶された識別情報とが同一であるかを判別するようにしてもよい。

【0015】また、上記通信端末において、前記受信手段は、通信端末において実行可能な、識別情報が付与されている端末用プログラムをネットワークを介して受信し、前記判別手段は、前記受信手段により受信された端末用プログラムを実行する場合に、当該プログラムの実行に伴ってアクセスすることが定められた電子機器から当該端末用プログラムに対応した電子機器用プログラムに付与されている識別情報を取得して、この識別情報と当該端末用プログラムに付与されている識別情報とが同一であるかを判別するようにしてもよい。

【0016】また、上記通信端末において、前記実行手段により実行された端末用プログラムによる処理過程において生じた前記電子機器に対するアクセス要求を前記電子機器に送信する送信手段をさらに有するようにしてもよい。

【0017】さらに、上記通信端末において、前記端末用プログラムに対して許容されたアクセスの種類が記憶されている許容アクセス記憶手段と、前記実行手段により実行された端末用プログラムによる処理過程において前記電子機器に対するアクセス要求が生じた場合に、前記許容アクセス記憶手段を参照して前記アクセス要求を許可する可否かを決定する決定手段と、前記決定手段により許可されたアクセス要求を前記電子機器に送信する送信手段とをさらに有するようにしてもよい。

【0018】また、この発明は、電子機器に記憶されているデータにアクセスする通信端末であって、当該通信端末において実行される端末用プログラムとこのプログラムの実行に伴って当該通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとをネットワークを介して受信する受信手段と、前記受信手段により受信された端末用プログラムを当該通信端末のメモリに記憶する記憶手段と、前記記憶手段により受信された電子機器用プログラムを前記電子機器に送信する送信手段とを有する通信端末を提供する。

【0019】また、上記通信端末において、前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであってもよい。

【0020】また、上記課題を解決するために、この発明は、通信端末に対して着脱自在であり、ユーザ情報が記憶されているユーザ識別モジュールであって、当該ユーザ識別モジュールが装着された通信端末から前記ユーザ情報に対するアクセス要求を受信する受信手段と、前記通信端末において実行されている端末用プログラムに対応したモジュール用プログラムに従って、前記受信手段により受信されたアクセス要求に応じた前記ユーザ情報に対するアクセス処理を実行する実行手段とを有するユーザ識別モジュールを提供する。

【0021】また、上記ユーザ識別モジュールにおいて、前記通信端末からの要求に応じて、当該ユーザ識別モジュールを特定する識別情報を前記通信端末に出力する出力手段をさらに有するようにしてもよい。

【0022】また、上記ユーザ識別モジュールにおいて、前記通信端末からの要求に応じて、前記通信端末において実行されている端末用プログラムに対応付けられたモジュール用プログラムを特定する特定手段と、前記特定手段により特定されたモジュール用プログラムに付与されている識別情報を前記通信端末に出力する出力手段とをさらに有するようにしてもよい。

【0023】また、この発明は、通信端末に対して着脱自在であり、ユーザ情報が記憶されているユーザ識別モジュールであって、当該ユーザ識別モジュールが装着された通信端末から当該通信端末を特定する識別情報と当該ユーザ識別モジュールにおいて実行可能なモジュール用プログラムとを対応付けて記憶する記憶手段と、当

該ユーザ識別モジュールが装着された通信端末から前記識別情報を受信する受信手段と、前記受信手段により受信された識別情報と前記記憶手段により記憶された識別情報とが同一であるかを判別する判別手段と、前記判別手段による判別結果を前記通信端末に出力する出力手段とを有するユーザ識別モジュールを提供する。

【0024】また、上記課題を解決するために、この発明は、サーバが、通信端末において実行される端末用プログラムと、当該プログラムの実行に伴って前記通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとをネットワークを介して通信端末に送信する第1の過程と、前記通信端末が、前記第1の過程にて送信された端末用プログラムと電子機器用プログラムとを受信し、前記端末用プログラムを当該通信端末のメモリに記憶する第2の過程と、前記通信端末が、前記第2の過程にて受信された電子機器用プログラムを前記電子機器に送信する第3の過程と、前記電子機器が、前記第3の過程にて送信された電子機器用プログラムを受信し、当該電子機器用プログラムを当該電子機器のメモリに記憶する第4の過程とを有するプログラムの提供方法を提供する。

【0025】また、上記プログラムの提供方法において、前記第2の過程は、前記通信端末が、前記第1の過程にて送信された端末用プログラムと電子機器用プログラムとを受信する第5の過程と、前記通信端末が、前記電子機器から当該電子機器を特定する識別情報を取得して、当該識別情報と前記第5の過程にて受信された端末用プログラムとを対応付けて当該通信端末のメモリに記憶する第6の過程とを有するようにしてもよい。

【0026】また、上記プログラムの提供方法において、前記第1の過程では、前記サーバが、通信端末において実行される端末用プログラムと、当該プログラムの実行に伴って前記通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとを含むパッケージをネットワークを介して送信する場合に、前記パッケージ毎に異なる識別情報を前記端末用プログラムおよび前記電子機器用プログラムの各々に付与して送信し、前記第2の過程では、前記通信端末が、前記第1の過程にて送信されたパッケージを受信し、当該パッケージに含まれる端末用プログラムを当該プログラムに対して付与された識別情報とともに当該通信端末のメモリに記憶し、前記第4の過程では、前記電子機器が、前記第3の過程にて送信された電子機器用プログラムを受信し、この電子機器用プログラムを当該プログラムに対して付与された識別情報とともに当該電子機器のメモリに記憶するようにしてもよい。

【0027】さらに、上記プログラムの提供方法において、前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであってもよい。

【0028】また、上記課題を解決するために、この発明は、通信端末において実行される端末用プログラムと、当該プログラムの実行に伴って前記通信端末によりアクセスされる電子機器において実行される電子機器用プログラムとが記憶されている記憶手段と、通信端末からの指示に応じて、前記記憶手段から読み出した端末用プログラムと電子機器用プログラムとをネットワークを介して前記通信端末に送信する送信手段とを有する送信装置を提供する。

【0029】また、上記送信装置において、前記送信手段が前記端末用プログラムと前記電子機器用プログラムとを含んだパッケージを送信する場合には、前記パッケージ毎に異なる識別情報を前記端末用プログラムおよび前記電子機器用プログラムの各々に付与する識別情報付与手段をさらに有するようにしてもよい。

【0030】また、上記送信装置において、前記電子機器は、前記通信端末に対して着脱自在な、ユーザ情報が記憶されたユーザ識別モジュールであってもよい。

【0031】

【発明の実施の形態】以下、図面を参照して本発明の実施形態について説明する。なお、各図において共通する部分には、同一の符号が付されている。また、かかる実施形態は本発明の一態様を示すものであり、この発明を限定するものではなく、本発明の範囲で任意に変更可能である。

【0032】なお、以下の実施形態では、本発明を移動通信システムに適用した場合について説明する。また、以下の実施形態においてアプリケーションプログラムとは、JavaアプレットやJavaアプリケーションなどのJavaプログラミング言語で記述されたアプリケーションプログラムを指す。

【0033】【A、第1実施形態】

【A-1、第1実施形態の構成】

<1、移動通信システムの構成>図1は、この発明の第1実施形態に係るコンテンツサーバ20、携帯電話機50およびUIM (User Identity Module: ユーザ識別モジュール) 60を含む移動通信システム10の構成を例示するブロック図である。同図に示されるように、移動通信システム10は、複数のコンテンツサーバ20と、インターネット30と、移動通信網40と、複数の携帯電話機50と、複数のUIM60とを有する。

【0034】なお、図1においては、図面が煩雑になることを防ぐために、移動通信システム10を構成する所定のコンテンツサーバ20、移動通信網40を構成する所定の基地局41、移動通信網40に収容される所定の携帯電話機50および当該携帯電話機50に着脱自在な所定のUIM60のみが示されている。

【0035】次に、図1に示された各装置について説明する。コンテンツサーバ20は、携帯電話機50に提供する情報を、例えばHTML (HyperText Markup Language)

形式のファイルデータとして記憶している。また、コンテンツサーバ20は、このファイルデータ内でタグにより指定されたJavaアプレットや、Javaアプリケーションなどのプログラムを記憶している。コンテンツサーバ20は、これらのファイルデータやアプリケーションプログラムをインターネット30及び移動通信網40を介して携帯電話機50に提供する。

【0036】移動通信網40は、図示を省略した移動パケット通信網および移動電話網を有する。ここで、移動パケット通信網は、パケット通信サービスを提供する網であり、ゲートウェイサーバを介してインターネット30に接続されている。また、移動電話網は、一般的な移動電話のサービスを提供する網である。また、基地局41は、移動通信網40の通信サービスエリア内に多数設置されており、各々の無線セルに在置する携帯電話機50と無線通信を行う。

【0037】携帯電話機50は、自機が在置する無線セルをカバーする基地局41と無線通信を行い、通話サービスやパケット通信サービスを受ける移動機である。この携帯電話機50は、WWW (World Wide Web) ブラウザの機能を有し、このブラウザ機能を利用してコンテンツサーバ20から提供されるWWWページ (コンテンツ) の内容を液晶画面に表示することができる。また、携帯電話機50は、HTMLファイルデータ内にタグ指定されたJavaアプレットをダウンロードして、このJavaアプレットをWWWブラウザの機能を利用して実行することができる。また、携帯電話機50は、コンテンツサーバ20からダウンロードしたJavaアプリケーションを実行することができる。

【0038】UIM60は、加入者情報が記憶されたモジュールであって、例えば、ICカード (スマートカードとも呼ばれる) の形態を有する。このUIM60は、携帯電話機50に対して着脱自在である。また、このUIM60は、マイクロプロセッサを有し、当該モジュール用のアプリケーションプログラムを実行することができる。なお、UIM60に記憶されている加入者情報とは、例えば、このUIM60の所有者の電話番号、クレジットカード番号、銀行の口座番号などの個人情報や、所有者の発呼、着呼、通話などの履歴情報、課金情報などのサービス利用情報である。

【0039】<2、コンテンツサーバの構成>図2は、図1に示されたコンテンツサーバ20のハードウェア構成を例示するブロック図である。同図に示されるように、コンテンツサーバ20は、メモリ201と、CPU (Central Processing Unit) 202と、通信インタフェース203とを有し、これらの各部はバス204によって接続されている。

【0040】メモリ201には、CPU202によって実行される各種プログラムや、携帯電話機50において解釈・実行されるHTMLファイルデータなどが格納さ

れている。また、このメモリ201には、アプリケーションプログラム格納領域201a（以下、AP格納領域201aと記載する）が設けられている。このAP格納領域201aには、携帯電話機50およびこれに装着されたUIM60にダウンロードすることが可能なアプリケーションプログラムが格納されている。

【0041】ここで、AP格納領域201aに格納されているアプリケーションプログラムとは、携帯電話機50においてUIM60内の加入者情報を参照して実行される、例えば、電子定期券や株のオンライントレード用のプログラムなどである。また、図3に示されるように、AP格納領域201aに格納されているアプリケーションプログラムは、携帯電話機50のCPUにより実行される本体用APと、この本体用APの実行中にUIM60のCPUにより実行されるモジュール用APとによって構成されている。

【0042】CPU202は、メモリ201に格納されている各種プログラムを実行することにより、バス204を介して接続されている装置各部を制御する。このCPU202は、携帯電話機50からのダウンロード要求に応じて、この要求に対応するHTMLファイルデータやアプリケーションプログラムをメモリ201から読み出して、通信インタフェース203を介して携帯電話機50に送信する。

【0043】通信インタフェース203は、インターネット30を介して当該コンテンツサーバ20と他の装置との間で行われるデータ通信を制御する回路である。

【0044】＜3. 携帯電話機の構成＞図4は、図1に示された携帯電話機50のハードウェア構成を例示するブロック図である。同図に示されるように、携帯電話機50は、無線通信部501と、操作部502と、通話処理部503と、表示部504と、UIMインタフェース505と、CPU506と、記憶部507とを有し、これらの各部はバス511によって接続されている。

【0045】無線通信部501は、アンテナ501aを備え、基地局41との間で行われる無線データ通信を制御する。この無線通信部501は、CPU506の制御の下、音声データやダウンロード要求などの各種データを搬送波に重畳し、この信号をアンテナ501aから基地局41に送信する。また、無線通信部501は、基地局41から自機宛てに送られてくる信号をアンテナ501aを介して受信し、これを復調して音声データやHTMLファイルデータ、アプリケーションプログラムなどを得る。

【0046】操作部502は、数字や文字、操作指示などを入力するための複数のキーを備え、これらのキーの操作に応じた操作信号をCPU506に出力する。通話処理部503は、例えば、マイクフオンやスピーカ、音声処理部などを有し、CPU506の制御の下、呼続／切断処理を含む通話処理を行う。表示部504は、

液晶表示パネルと、この液晶表示パネルの表示制御を行う駆動回路とを有する。UIMインタフェース505は、当該携帯電話機50に装着されたUIM60との間で行われるデータ通信を制御する回路である。

【0047】記憶部507は、ROM（Read Only Memory）508と、RAM（Random Access Memory）509と、例えば、SRAM（Static-RAM）やEEPROM（Electrically Erasable Programmable Read Only Memory）などの不揮発性メモリ510とを有する。

【0048】ROM508には、CPU506によって実行される各種プログラムなどが格納されている。例えば、ROM508には、携帯電話機50用のオペレーティングシステム（以下、OSと略称する）やWWWブラウザのプログラム、Javaプログラミング言語で記述されたプログラムを当該携帯電話機50において実行するためのJava実行環境（以下、JREと略称する）のソフトウェアなどが格納されている。

【0049】RAM509は、CPU506のワークエリアとして用いられ、例えば、コンテンツサーバ20からダウンロードされたHTMLファイルデータやアプリケーションプログラムなどが一時的に格納される。

【0050】不揮発性メモリ510は、シリアルナンバー格納領域510aと、AP格納領域510bとを有する。シリアルナンバー格納領域510aには、携帯電話機50毎に固有のシリアルナンバー（製造番号）が、例えば工場出荷時に書き込まれる。また、AP格納領域510bには、コンテンツサーバ20からダウンロードされたアプリケーションプログラムのうち本体用APが格納される。ここで、図5に示されるように、AP格納領域510bに格納される本体用APは、ダウンロードされた時点において当該携帯電話機50に装着されているUIM60のシリアルナンバーと対応付けられて格納される。

【0051】CPU506は、記憶部507に格納されている各種プログラムを実行することにより、バス511を介して接続されている装置各部を制御する。このCPU506は、本実施形態に特有な処理として、後述するダウンロード処理（図9参照）およびアクセス管理処理（図10参照）を実行する。

【0052】＜4. UIMの構成＞図6は、図1に示されたUIM60のハードウェア構成を例示するブロック図である。同図に示されるように、UIM60は、外部インタフェース601と、ROM602と、RAM603と、CPU604と、EEPROM605とを有し、これらの各部はバス606によって接続されている。

【0053】外部インタフェース601は、携帯電話機50との間で行われるデータ通信を制御する回路である。

【0054】ROM602には、CPU604によって実行される各種プログラムなどが格納されている。例え

15

ば、ROM602には、UIM60用のOSや、Javaプログラミング言語で記述されたプログラムを当該UIM60において実行するためのJavaカード実行環境（以下、JCREと略称する）のソフトウェア、携帯電話機50から受信したモジュール用APをEEPROM605に格納するローダのプログラムなどが格納されている。

【0055】RAM603は、CPU604のワークエリアとして用いられ、例えば、携帯電話機50から受信したモジュール用APなどが一時的に格納される。

【0056】EEPROM605は、シリアルナンバー格納領域605aと、AP格納領域605bと、加入者情報格納領域605cとを有する。シリアルナンバー格納領域605aには、UIM60毎に固有のシリアルナンバーが、例えば工場出荷時に書き込まれる。また、AP格納領域605bには、携帯電話機50から受信したモジュール用APが格納される。ここで、図7に示されるように、AP格納領域605bに格納されるモジュール用APは、このモジュール用APがダウンロードされた時点において当該UIM60が装着されている携帯電話機50のシリアルナンバーと対応付けられて格納される。また、加入者情報格納領域605cには、前述した個人情報やサービス利用情報などの加入者情報が格納されている。

【0057】CPU604は、ROM602やEEPROM605に格納されている各種プログラムを実行することにより、バス606を介して接続されている各部を制御する。このCPU604は、本実施形態に特有な処理として、後述するダウンロード処理（図9参照）およびアクセス管理処理（図10参照）を実行する。

【0058】＜5. アプリケーションプログラムの実行環境＞図8は、本体用APとモジュール用APの実行環境を例示する模式図である。同図左側に示される機能階層モデルは、携帯電話機50における本体用APの実行環境を示すものであり、同図右側に示される機能階層モデルは、UIM60におけるモジュール用APの実行環境を示すものである。

【0059】まず、同図左側の本体用APの実行環境を示す機能階層モデルは、最下層から上層位に向かって順に、OS（携帯電話機50用）と、Javaアプリケーションマネージャ（以下、JAMと略称する）と、Javaバーチャルマシン（以下、JavaVMと略称する）と、複数の本体用APとを有する。

【0060】ここで、OSは、携帯電話機50の基本的な制御を司る機能を有する。JAMは、各本体用APの実行に関するセキュリティなどを管理する機能を有する。また、JavaVMは、JAMによる制御の下、本体用APを実行するための機能を有し、Javaの実行ファイル形式であるバイトコードを携帯電話機50のCPU506がOSを介して解釈可能な命令コードに変換する。J

16

AMおよびJavaVMは、JREに組み込まれており、携帯電話機50のROM508に記憶されている。

【0061】次に、同図右側のモジュール用APの実行環境を示す機能階層モデルは、最下層から上層位に向かって順に、OS（UIM60用）と、Javaカードバーチャルマシン（以下、Java Card VMと略称する）およびローダと、複数のモジュール用APとを有する。

【0062】ここで、OSは、UIM60の基本的な制御を司る機能を有する。このOSには、UIM60内の各モジュール用APの格納の有無を確認したり、携帯電話機50から受信したアクセス要求などのモジュール用APに引き渡すのかを判断するカードマネージャの機能が含まれる。また、Java Card VMは、モジュール用APを実行するための機能を有し、JavaのバイトコードをUIM60のCPU604がOSを介して解釈可能な命令コードに変換する。このJava Card VMは、JCREに組み込まれており、UIM60のROM602に記憶されている。また、ローダは、携帯電話機50から受信したデータやプログラムをEEPROM605にインストールする機能を有し、OS上で実行される。

【0063】なお、UIM60において各モジュール用APは、Java Card VMの仕様により、原則として当該アプリケーションが管理する加入者情報にしかアクセスできない構成となっている。

【0064】次に、この図8に基づいて、携帯電話機50からUIM60内の加入者情報に対してアクセスする場合の動作を説明する。携帯電話機50のCPU506は、本体用APによる処理過程においてUIM60内の加入者情報に対するアクセス要求が生じると、まず、JAMに従ってこのアクセス要求がセキュリティを確保する上で許容されるものであるか否かを判断する。その結果、アクセス要求が許容された場合、このアクセス要求がJavaVMによりCPU506で解釈可能な命令コードに変換される。

【0065】ここで、アクセス要求には、アクセスコマンドとコマンド関連データとが含まれる。アクセスコマンドとは、例えば、読み出し、書き換え、削除など、加入者情報に対するアクセスの種類を示すものである。また、コマンド関連データとは、例えば、書き換えるデータを指定する情報や書き換え用のデータ、読み出すデータを指定する情報などである。CPU506は、OSに従ってこのアクセスコマンドとコマンド関連データとを含むアクセス要求をUIMインタフェース505経由でUIM60に送信する。

【0066】UIM60のCPU604は、外部インタフェース601を介してアクセス要求を受信すると、まず、OS内のカードマネージャに従ってアクセス要求を引き渡すモジュール用APを特定する。次いで、このモジュール用APがJava Card VM上において起動される。そして、CPU604は、このモジュール用APに

従って、アクセス要求に応じた加入者情報に対する読み出しや書き換え、削除などのアクセス処理を実行する。

【0067】なお、図8左側に示された本体用APの実行環境を示す機能階層モデルにおいて、JavaVMは、KVM(K Virtual Machine)などであってもよい。以上が本実施形態に係る移動通信システム10の構成である。

【0068】[A-2、第1実施形態の動作] 次に、本実施形態の動作について説明する。

<1. ダウンロード処理>

【0069】携帯電話機50は、操作入力に応じてWWWページの閲覧モードが指示された場合に、ROM508からWWWブラウザのプログラムを読み出して実行する。そして、所望のコンテンツサーバ20からインターネット30および移動通信網40を介してダウンロードされたHTMLファイルデータに基づいて、表示画面にWWWページの内容を表示する。ユーザがこのWWWページの閲覧中に携帯電話機50に対してアプリケーションプログラムのダウンロードを操作入力により指示すると、以下に説明するダウンロード処理が開始される。

【0070】図9は、コンテンツサーバ20からアプリケーションプログラムをダウンロードする場合の、コンテンツサーバ20、携帯電話機50およびUIM60の動作を示すシーケンスチャートである。

【0071】同図に示されるように、まず、携帯電話機50のCPU506は、ダウンロード要求をコンテンツサーバ20に送信する(ステップS101)。このダウンロード要求には、ダウンロードを指示するコマンドとダウンロードするアプリケーションプログラムを指定する情報とが含まれる。

【0072】コンテンツサーバ20のCPU202は、携帯電話機50からダウンロード要求を受信すると、このダウンロード要求に応じたアプリケーションプログラムをAP格納領域201aから読み出す(ステップS102)。ここで読み出されるアプリケーションプログラムとは、図3に示されたように、ペダとして対応付けられている本体用APおよびモジュール用APである。そして、CPU202は、この本体用APおよびモジュール用APを1つのパッケージとして携帯電話機50にダウンロードする(ステップS103)。なお、コンテンツサーバ20から携帯電話機50にダウンロードされるパッケージに対しては、圧縮処理や暗号化処理が施されているともよい。

【0073】携帯電話機50のCPU506は、コンテンツサーバ20からパッケージをダウンロードすると、図8に示されたJAMに従って、以下のステップS104～S107の処理を行う。

【0074】すなわち、まず、CPU506は、ダウンロードしたパッケージに対する認証処理を行う(ステップS104)。この認証処理は、例えば、電子署名など

によって、ダウンロードしたパッケージの正当性を確認する処理である。この認証処理の後、CPU506は、ダウンロードされたパッケージから本体用APおよびモジュール用APを取り出す(ステップS105)。そして、CPU506は、モジュール用APとシリアルナンバー格納領域510aから読み出した当該携帯電話機50のシリアルナンバー(本体シリアルナンバー)とをUIM60に送信する(ステップS106)。なお、携帯電話機50からUIM60に送信されるデータに対しては、暗号化処理が施されているともよい。

【0075】また、CPU506は、上記ステップS106において取り出した本体用APを、現時点において携帯電話機50に装着されているUIM60のシリアルナンバー(モジュールシリアルナンバー)と対応付けてAP格納領域510bに格納する(ステップS107)。なお、モジュールシリアルナンバーは、UIM60が携帯電話機50に装着された時点でUIM60から携帯電話機50に送信され、RAM509に格納されている。

【0076】一方、UIM60のCPU604は、上記ステップS106において携帯電話機50からモジュール用APおよび本体シリアルナンバーを受信すると、まず、OS内のローダを起動する。そして、CPU604は、このローダに従って当該モジュール用APを本体シリアルナンバーと対応付けてAP格納領域510bに格納する(ステップS108)。この後、CPU604は、インストールが完了したことを示すインストール完了通知を携帯電話機50に送信する(ステップS109)。これにより当該ダウンロード処理が終了する。

【0077】以上説明したようにダウンロード処理では、本体用APおよびモジュール用APがコンテンツサーバ20から携帯電話機50に一括してダウンロードされる。したがって、ダウンロードに要する通信時間や通信コストを低減することができる。

【0078】<2. アクセス管理処理>図10は、携帯電話機50がUIM60内の加入者情報にアクセスする場合の、携帯電話機50およびUIM60の動作を示すシーケンスチャートである。このアクセス管理処理は、携帯電話機50において本体用APの実行が指示された場合に開始される。

【0079】携帯電話機50のCPU506は、まず、JAMに従って、以下のステップS201～S203の処理を行う。すなわち、CPU506は、指示された本体用APを実行する前に、この本体用APとこれに対応するモジュール用APの認証を行うために、まず、実行が指示された本体用APの識別情報(例えば、ファイル名)を取得する(ステップS201)。また、シリアルナンバー格納領域510aから本体シリアルナンバーを読み出す(ステップS202)。そして、CPU506は、取得した識別情報および本体シリアルナンバーをU

IM60に送信する(ステップS203)。

【0080】UIM60のCPU604は、携帯電話機50から識別情報および本体シリアルナンバーを受信すると、OS内のカードマネージャに従って、以下のステップS204～S206の処理を行う。すなわち、CPU604は、受信した識別情報に従って、この本体用APに対応するモジュール用APがAP格納領域605bに格納されているか否かを確認する(ステップS204)。また、シリアルナンバー格納領域605aからモジュールシリアルナンバーを読み出す(ステップS205)。そして、CPU604は、格納有無の結果およびモジュールシリアルナンバーを携帯電話機50に送信する(ステップS206)。

【0081】携帯電話機50のCPU506は、UIM60から格納有無の結果およびモジュールシリアルナンバーを受信すると、JAMに従い、プログラムの実行が指示された本体用APとこれに対応するモジュール用APとの認証処理を行う(ステップS207)。

【0082】本実施形態において、本体用APとモジュール用APとの認証処理とは、実行が指示された本体用APに対応するモジュール用APがUIM60に格納されていること、および現時点における携帯電話機50とこれに装着されたUIM60の組み合わせが、この本体用APおよびモジュール用APをダウンロードした時の携帯電話機50とUIM60の組み合わせと同一であること、の二点を確認することである。

【0083】CPU506は、上記ステップS207に示す認証処理として、UIM60から送信されたモジュール用APの格納有無の結果に従って、実行が指示された本体用APに対応するモジュール用APがUIM60に格納されているか否かを確認する。また、CPU506は、UIM60から送信されたモジュールシリアルナンバーと、実行が指示された本体用APと対応付けられてAP格納領域510bに格納されているモジュールシリアルナンバーとを比較することにより、携帯電話機50とUIM60の組み合わせがこの本体用APおよびモジュール用APをダウンロードした時の組み合わせと同一であるか否かを確認する。

【0084】一方、UIM60のCPU604においても、カードマネージャに従い、本体用APとモジュール用APとの認証が行われ(ステップS208)、認証結果が携帯電話機50に通知される(ステップS209)。ここで、上記ステップS208において行われる認証処理は、携帯電話機50側で行われる認証処理と同様である。

【0085】すなわち、CPU604は、上記ステップS204において判別したモジュール用APの格納有無の結果に従って、プログラムの実行が指示された本体用APに対応するモジュール用APが当該UIM60に格納されているか否かを確認する。また、CPU604

は、携帯電話機50から送信された本体シリアルナンバーと、実行が指示された本体用APに対応するモジュール用APに対応付けられてAP格納領域605bに格納されているモジュールシリアルナンバーとを比較することにより、携帯電話機50とUIM60の組み合わせがこの本体用APおよびモジュール用APをダウンロードした時の組み合わせと同一であるか否かを確認する。

【0086】このようにして携帯電話機50とUIM60との双方で認証処理が行われた後、携帯電話機50のCPU506は、JAMに従い、相互認証が成立したか否かを判別する(ステップS210)。その結果、相互認証が成立しなかった場合、CPU506は、認証が不成立であった旨のメッセージを画面表示し、本体用APの実行をキャンセルする(ステップS211)。また、これにより当該アクセス管理処理が終了する。

【0087】なお、相互認証が成立しなかった場合とは、具体的には、プログラムの実行が指示された本体用APに対応するモジュール用APがUIM60に格納されていなかった場合や、携帯電話機50とUIM60の組み合わせがこの本体用APおよびモジュール用APをダウンロードした時の組み合わせと異なる場合などである。

【0088】一方、CPU506は、上記ステップS210において相互認証が成立したと判別した場合には、まず、実行が指示された本体用APをJavaVM上において起動し、当該本体用APの処理を開始する(ステップS212)。次いで、CPU506は、本体用APによる処理過程においてUIM60内の加入者情報に対するアクセス要求が発生すると(ステップS213)、JAMに従って、このアクセス要求がセキュリティを確保する上で許容されるものであるか否かを判別する(ステップS214)。

【0089】そして、CPU506は、アクセス要求が許容された場合、前述したアクセスコマンドおよびコマンド関連情報②、当該本体用APの識別情報①を含むアクセス要求をUIM60に送信する(ステップS215)。

【0090】なお、CPU506は、上記ステップS213においてアクセス要求が発生していない場合や、上記ステップS214においてアクセス要求が許容されないものであった場合には、ステップS219の処理に移行する。また、上記ステップS214においてアクセス要求が許容されないものであった場合には、許容不可のアクセスが発生したことを示すメッセージを画面表示し、本体用APの実行を中止する構成としてもよい。

【0091】UIM60のCPU604は、上記ステップS215において携帯電話機50からアクセス要求を受信すると、カードマネージャに従い、対応するモジュール用APを特定する。そして、CPU604は、Java Card VM上においてこのモジュール用APを実行する

(ステップS216)。

【0092】次いで、CPU604は、このモジュール用APに従い、携帯電話機50からのアクセス要求に応じた加入者情報に対する読み出しや書き換え、削除などのアクセス処理を実行する(ステップS216)。このアクセス処理が終了すると、CPU604は、アクセス処理が完了したことを示すアクセス完了通知を携帯電話機50に送信する(ステップS218)。なお、アクセス要求が加入者情報の読み出しであった場合は、読み出された加入者情報がアクセス完了通知に含まれて携帯電話機50に送信される。

【0093】携帯電話機50のCPU506は、UIM60からアクセス完了通知を受信すると、本体用APの処理を終了するか否かを判別し(ステップS219)、終了でなければ上記ステップS213に戻り、本体用APの処理を継続する。また、終了であれば、本体用APの処理を終了する。これにより当該アクセス管理処理が終了する。

【0094】以上説明したように本実施形態によれば、携帯電話機50のCPU506は、コンテンツサーバ20からインターネット30を介して取得した本体用APの実行が指示されると、当該携帯電話機50に装着されたUIM60からモジュールシリアルナンバーを取得し、本体用APに対応付けられたモジュールシリアルナンバーと比較する。これによりCPU506は、現時点における携帯電話機50とUIM60の組み合わせが、この本体用APをダウンロードした時点における携帯電話機50とUIM60の組み合わせと同一であるか否かを判別する。

【0095】そして、CPU506は、現時点における携帯電話機50とUIM60の組み合わせが、この本体用APをダウンロードした時点における携帯電話機50とUIM60の組み合わせと同一であると判別した場合に、本体用APを実行する。そして、この本体用APによる処理過程においては、本体用APおよびこれに対応するUIM60内のモジュール用APが連携して動作することにより、携帯電話機50からUIM60に格納されている加入者情報へのアクセスが行われる。

【0096】つまり、本体用APの実行時における携帯電話機50とUIM60の組み合わせがこの本体用APをダウンロードした時点における携帯電話機50とUIM60の組み合わせと異なる場合や、本体用APに対応するモジュール用APがUIM60に格納されていなかった場合などは、本体用APの実行がキャンセルされ、携帯電話機50は、UIM60内の加入者情報にアクセスすることができない。

【0097】このように、インターネット30を介して取得した本体用APの実行については、携帯電話機50とUIM60との間で上述した一定の条件が成立した場合のみ実行が許可され、携帯電話機50からUIM60

0内の加入者情報へのアクセスが可能となる。したがって、携帯電話機50は、インターネット30を介して取得したプログラムの実行に際し、セキュリティを確保しつつ、このプログラムに従って当該携帯電話機50外の、UIM60に格納されている加入者情報にアクセスすることができる。

【0098】[A-3. 具体的な適用例] 以下に本発明を適用したアプリケーションプログラムの概要を説明する。

<1. 電子定期券アプリケーション>本発明を電子定期券のアプリケーションプログラムに適用した場合について説明する。この場合、UIM60には、加入者情報としてさらに、利用者氏名や利用区間、有効期間などの定期券情報が格納されている。また、携帯電話機50は、例えば、Home RF (Home Radio Frequency) やBluetooth (登録商標) などにより改札に設置された利用者の通過許可を判断する制御装置との間で近距離の無線通信を行う近距離無線通信部をさらに有する。

【0099】改札を通過する際、携帯電話機50およびこれに装着されたUIM60では、電子定期券用の本体用APとモジュール用APとの相互認証が行われる。そして、相互認証が成立した後、携帯電話機50のCPU506は、電子定期券用の本体用APを起動し、改札に設置された制御装置からの信号を受信する。次いで、CPU506は、この信号の受信に応じて、定期券情報の読み出しを指示するアクセス要求をUIM60に送信する。

【0100】UIM60のCPU60は、アクセス要求の受信に応じて電子定期券用のモジュール用APを起動し、当該モジュール用APに従ってUIM60内の定期券情報を読み出して携帯電話機50に送信する。携帯電話機50のCPU506は、UIM60から定期券情報を受信すると、この定期券情報を近距離無線通信部により制御装置に送信する。そして、改札に設置された制御装置は、受信した定期券情報に従って、この携帯電話機50を所持する利用者の通過許可を決定する。

【0101】<2. 決済アプリケーション>次に、本発明を決済処理のアプリケーションプログラムに適用した場合について説明する。この場合、UIM60には、加入者情報としてクレジットカード番号や銀行の口座番号などの決済に使用する決済使用情報が格納されている。

【0102】インターネット30に接続されているサーバやPOS (Point Of Sales) などの端末と通信を行って商品の売買契約を行い、代金支払いの決済を行う場合、携帯電話機50およびこれに装着されているUIM60では、決済処理用の本体用APとモジュール用APとの相互認証が行われる。そして、相互認証が成立した後、携帯電話機50のCPU506は、決済処理用の本体用APを起動して決済方法の選択メニューを画面表示し、ユーザに選択を促す。これに応じてユーザは、キー

操作により決済方法を選択する。次いで、CPU506は、ユーザにより選択された決済方法に該当する決済使用情報の読み出しを指示するアクセス要求をUIM60に送信する。

【0103】UIM60のCPU60は、アクセス要求の受信に応じて決済処理用のモジュール用APを起動し、当該モジュール用APに従って該当する決済使用情報の読み出しを携帯電話機50に送信する。携帯電話機50のCPU506は、UIM60から決済使用情報を受信すると、この決済使用情報を液晶画面に表示する。

そして、ユーザにより暗証番号情報などがキー操作によって入力され、最終的な決済の指示が決定されると、携帯電話機50は、暗証番号情報などを含んだ決済使用情報を暗号化してPOSなどの相手先装置に送信する。これにより相手先装置と決済センタや金融機関の決済サーバとの間で商品の売買契約に伴う決済処理が行われる。

【0104】[B. 第2実施形態] 上記第1実施形態では、携帯電話機50から当該携帯電話機50に装着されたUIM60内の加入者情報に対してアクセスする場合について説明した。本実施形態では、携帯電話機からパーソナルコンピュータなどの電子機器に記憶されたデータに対してアクセスする場合について説明する。

【0105】なお、本実施形態において、上記第1実施形態と共通する部分については同一の符号を使用するものとする。また、上記第1実施形態と共通する部分についてはその説明を省略するものとする。

【0106】[B-1. 第2実施形態の構成] 図11は、第2実施形態に係る携帯電話機55のハードウェア構成を例示するブロック図である。図11において上記第1実施形態の携帯電話機50と異なるのは、UIMインタフェース505の代わりに赤外線通信部550が設けられ、この赤外線通信部550を介して当該携帯電話機55が電子機器70とデータ通信を行うことが可能な点である。

【0107】赤外線通信部550は、赤外線通信（例えば、IrDA (Infrared Data Association) 規格に従った通信）により電子機器70との間で行われるデータ通信を制御する。

【0108】電子機器70は、例えば、パーソナルコンピュータやPDAなどであり、上述した赤外線通信機能を有している。また、この電子機器70は、Javaプログラミング言語で記述されたプログラムの実行環境（JRE）を有している。ここで、この電子機器70におけるJavaプログラムの実行環境は、上記第1実施形態におけるUIM60の場合と異なり、Java Card VMの代わりにJAMとJavaVMとを有する。また、この電子機器70内のメモリには、例えば、この電子機器70の所有者の氏名やクレジットカード番号などの個人情報格納されている。

【0109】本実施形態においてコンテンツサーバ20

から携帯電話機55および電子機器70にダウンロードされるアプリケーションプログラムは、携帯電話機55のCPU506により実行される端末用APと、電子機器70のCPUにより実行される電子機器用APとによって構成されている。また、電子機器用APは、コンテンツサーバ20から携帯電話機55を経由して電子機器70にダウンロードされる。

【0110】また、本実施形態における携帯電話機55は、アクセス先の電子機器を特定する情報として、コンテンツサーバ20からダウンロードした電子機器用APを電子機器70へ送信した際に、この電子機器70とのデータ通信に使用した当該携帯電話機55の入出力ポート番号を端末用APと対応付けて不揮発性メモリ510に格納する。また、不揮発性メモリ510のAP格納領域510bには、電子機器用APをダウンロードした電子機器70から取得した当該電子機器70のシリアルナンバーが端末用APと対応付けられて格納される。

【0111】[B-2. 第2実施形態の動作] 次に、本実施形態の動作について説明する。本実施形態において携帯電話機55および電子機器70は、上記第1実施形態において説明したダウンロード処理（図9参照）と同様の処理を実行する。そして、このダウンロード処理において携帯電話機55からの操作入力によって指定されたコンテンツサーバ20内の端末用APおよび電子機器用APは、インターネット30を介して携帯電話機55にダウンロードされる。

【0112】携帯電話機55は、まず、電子機器用APを送信する電子機器70から当該電子機器70のシリアルナンバーを赤外線通信部550経由で取得して、当該シリアルナンバーとダウンロードした端末用APとを対応付けてAP格納領域510bに格納する。また、携帯電話機55は、電子機器70とのデータ通信に使用した当該携帯電話機55の入出力ポート番号、この端末用APの処理過程においてアクセスする電子機器の特定情報として、端末用APと対応付けて不揮発性メモリ510に格納する。

【0113】次いで、携帯電話機55は、シリアルナンバー格納領域510aに格納されている自機のシリアルナンバーを読み出して、当該シリアルナンバーとダウンロードした電子機器用APとを赤外線通信部550により電子機器70に送信する。電子機器70では、受信した携帯電話機55のシリアルナンバーと電子機器用APとを対応付けてメモリに格納する。

【0114】そして、携帯電話機55および電子機器70は、上記第1実施形態において説明したアクセス管理処理（図10参照）と同様の処理を実行し、プログラムの実行が指示された端末用APおよびこれに対応する電子機器用APの相互認証を行う。そして、相互認証された端末用APおよび電子機器用APが連携して動作することにより、携帯電話機55から電子機器70内の個人

情報に対するアクセス処理が行われる。

【0115】より具体的に説明すると、まず、ユーザは、アクセス先となる電子機器70を操作して、当該電子機器70が携帯電話機55と赤外線通信を行うことが可能な状態とする。次いで、ユーザは、携帯電話機55に対して、端末用APの実行を指示する操作入力を行う。これに応じて携帯電話機55のCPU506は、実行が指示された端末用APと対応付けて不揮発性メモリ510に格納している入出力ポート番号（アクセス先の電子機器を特定する情報）を読み出す。

【0116】次いで、携帯電話機55は、読み出した入出力ポート番号に従って赤外線通信部550を選択し、当該携帯電話機55と赤外線通信を行うことが可能な状態にある電子機器を特定するための呼出し信号を赤外線通信部550から送信する。そして、携帯電話機55は、この呼出し信号に対して応答信号を返信してきた電子機器70を特定する。

【0117】次いで、携帯電話機55のCPU506は、特定した電子機器70から当該電子機器70のシリアルナンバーを赤外線通信部550経由で取得し、端末用APに対応付けられているシリアルナンバーと比較する。これによりCPU506は、現時点において携帯電話機55と赤外線通信を行っている電子機器70がこの端末用APとペアになる電子機器用APをダウンロードした電子機器70であるかを判断する。

【0118】そして、CPU506は、携帯電話機55と赤外線通信を行っている電子機器70が実行指定された端末用APとペアになる電子機器用APをダウンロードした電子機器70であると判断した場合に、端末用APを実行する。この端末用APによる処理過程においては、端末用APおよびこれに対応する電子機器70内の電子機器用APが連携して動作することにより、携帯電話機55から電子機器70のメモリに格納されている加入者情報へのアクセスが行われる。

【0119】つまり、端末用APの実行時において、携帯電話機55と赤外線通信を行っている電子機器70が端末用APとペアになる電子機器用APをダウンロードした電子機器70と異なる場合や、この電子機器70に端末用APに対応する電子機器用APが格納されていない場合などは、端末用APの実行がキャンセルされ、携帯電話機55は、電子機器70内の加入者情報にアクセスすることができない。

【0120】このように、インターネット30を介して取得した端末用APの実行については、携帯電話機55と電子機器70の間で上述した一定の条件が成立した場合のみ実行が許可され、これにより携帯電話機55から電子機器70内の加入者情報へのアクセスが可能となる。したがって、携帯電話機55は、インターネット30を介して取得したプログラムの実行に際し、セキュリティを確保しつつ、このプログラムに従って当該携

電話機55外の、当該携帯電話機55と赤外線通信を行うことが可能な電子機器70内のメモリに記憶されている個人情報にアクセスすることができる。

【0121】なお、本実施形態では、携帯電話機55が電子機器70との間で赤外線通信を行う場合について説明した。しかしながら、赤外線通信の代わりに、例えば、HomeRFやBluetooth（登録商標）を用いてもよい。また、通信ケーブルにより携帯電話機55と電子機器70とが有線接続される場合に対しても本発明が適用可能であることは勿論である。

【0122】また、アクセス対象は個人情報に限定されず、電子機器70内のその他の格納データであってもよい。さらに、携帯電話機55から電子機器70へのアクセスは、データ以外の、例えば、電子機器70に格納されているプログラムの起動であってもよい。また、電子機器70内の入出力ポートへのアクセスなどであってもよい。

【0123】〔C. 変形例〕以上、本発明の実施形態について説明したが、この実施形態はあくまでも例示であり、本発明の趣旨から逸脱しない範囲で様々な変形が可能である。変形例としては、例えば以下のようなものが考えられる。

【0124】＜変形例1＞上記第1実施形態では、本体用APおよびモジュール用APをコンテンツサーバ20から一括してダウンロードする場合について説明した。しかしながら、ダウンロードの手順は、例えば、図12に示されるような手順であってもよい。図12は、コンテンツサーバ20からアプリケーションプログラムをダウンロードする場合の変形例について示すシーケンスチャートである。なお、以下の説明では、上記実施形態で述べたダウンロード処理（図9参照）と異なる部分を中心に説明を行う。

【0125】図12に示されるように、まず、携帯電話機50のCPU506は、ダウンロード要求をコンテンツサーバ20に送信する（ステップS301）。コンテンツサーバ20のCPU202は、携帯電話機50からダウンロード要求を受信すると、このダウンロード要求に応じた本体用APをAP格納領域201aから読み出す（ステップS302）。そして、CPU202は、本体用APのみを携帯電話機50にダウンロードする（ステップS303）。

【0126】携帯電話機50のCPU506は、コンテンツサーバ20から本体用APをダウンロードすると、まず、JAMに従い、ダウンロードした本体用APの認証処理を行う（ステップS304）。この認証処理は、例えば、電子署名などによりダウンロードした本体用APの正当性を確認する処理である。この認証処理の後、CPU506は、JAMに従って本体用APを当該携帯電話機50に装填されているUIM60のモジュールシリアルナンバーと対応付けてAP格納領域510bに格

納する(ステップS305)。次いで、CPU506は、格納した本体用APに対応するモジュール用APのダウンロード要求をコンテンツサーバ20に送信する(ステップS306)。

【0127】コンテンツサーバ20のCPU202は、携帯電話機50からのダウンロード要求に応じたモジュール用APをAP格納領域201aから読み出す(ステップS307)。そして、CPU202は、モジュール用APを携帯電話機50にダウンロードする(ステップS308)。

【0128】携帯電話機50のCPU506は、コンテンツサーバ20からモジュール用APをダウンロードすると、JAMに従ってモジュール用APの認証処理を行う(ステップS309)。その後、CPU506は、JAMに従ってモジュール用APと当該携帯電話機50の本体シリアルナンバーとをUIM60に送信する(ステップS310)。

【0129】UIM60のCPU604は、モジュール用APおよび本体シリアルナンバーを受信すると、OS内のローダに従って、当該モジュール用APを本体シリアルナンバーと対応付けてAP格納領域510bに格納する(ステップS311)。その後、UIM60から携帯電話機50にインストール完了通知が送信され(ステップS312)、ダウンロード処理が終了する。

【0130】以上説明したようにダウンロード処理は、本体用APとモジュール用APとをコンテンツサーバ20から別々にダウンロードする構成であってもよい。

【0131】<変形例2>上記第1実施形態および変形例1では、本体用APおよびモジュール用APをコンテンツサーバ20からダウンロードする場合について説明した。しかしながら、本発明は、本体用APおよびモジュール用APをコンテンツサーバ20から各携帯電話機50に配信する場合についても適用可能である。

【0132】この場合、コンテンツサーバ20は、配信先となる携帯電話機50の通信アドレス(例えば、IPアドレスやメールアドレスなど)が登録された配信優先リストを有する。そして、コンテンツサーバ20は、送信すべき本体用APおよびモジュール用APを(上述した)配信優先リストに登録されている携帯電話機50およびこれに装着されたUIM60に配信する。

【0133】<変形例3>上記第1実施形態では、アクセス管理処理において、プログラムの実行が指示された本体用APとこれに対応するモジュール用APとの認証処理を行うために、本体シリアルナンバーおよびモジュールシリアルナンバーを用いる構成とした。

【0134】しかしながら、例えば、コンテンツサーバ20から本体用APおよびモジュール用APを送信する際に、送信するパッケージ毎に異なる識別情報を本体用APおよびモジュール用APの両方に付与し、この識別情報を本体シリアルナンバーおよびモジュールシリアル

ナンバーの代わりに用いる構成としてもよい。

【0135】この場合、ダウンロードされた本体用APやモジュール用APは、コンテンツサーバ20によって付与された識別情報と対応付けられ(携帯電話機50のAP格納領域510bまたはUIM60のAP格納領域605bに格納される。そして、アクセス管理処理において本体用APとモジュール用APとの認証処理を行う場合、携帯電話機50のCPU506は、プログラムの実行が指示された本体用APに対応付けられている識別情報と、この本体用APに対応するモジュール用APに対応付けられている識別情報とが同一であるか否かを照合する。

【0136】このような構成とすれば、本体用APとモジュール用APとが同一のパッケージでダウンロードされたプログラムであるか否かに基づいて脱脱を行うことができる。また、本変形例において説明した内容は、ダウンロードの場合のみでなく、配信の場合に対しても適用可能であることは勿論である。

【0137】<変形例4>上記第1実施形態において、さらに以下に述べる制御を行う構成としてもよい。すなわち、コンテンツサーバ20は、図13に示されるように、各本体用AP毎に、当該本体用APがUIM60内の加入者情報に対して実行可能なアクセス行為を規定したアクセス規定データをメモリ201に記憶している。そして、コンテンツサーバ20は、本体用APおよびモジュール用APをダウンロード(または配信)する際に、本体用APとともにこれに対応するアクセス規定データを携帯電話機50にダウンロードする。携帯電話機50では、ダウンロードされた本体用APとアクセス規定データとを対応付けて不揮発性メモリ510に格納する。

【0138】そして、携帯電話機50のCPU506は、アクセス管理処理においてアクセス要求が許容アクセスであるか否かを判断する際に(ステップS214)、プログラムの実行が指示された本体用APに対応するアクセス規定データを参照してアクセス要求の可否を決定する。

【0139】なお、図13に示されたアクセス規定データにおいて、「許可」項目では、「1」が対応するアクセス行為の許可を、「0」が不許可を示す。また、このアクセス規定データにおけるアクセス行為の可否は、JavaアプレットやJavaアプリケーションにおける「メソッド」単位で設定される構成であってもよい。例えば、Aメソッドは許可、Bメソッドは不許可など、メソッドの種類に応じてアクセス行為の可否を設定してもよい。

【0140】このような構成とすれば、加入者情報に対するアクセスの種類に応じてアクセス要求の可否を決定することができる。

【0141】<変形例5>上記第1実施形態では、本体用APの実行が指示されると、当該本体用APとこれに

対応するモジュール用ＡＰとの認証を行う構成とした。しかしながら、例えば、以下に述べる制御構成であってもよい。

【０１４２】すなわち、携帯電話機５０に対してＵＩＭ６０が装着されると、この時点で、携帯電話機５０に格納されている各本体用ＡＰと、ＵＩＭ６０に格納されている各モジュール用ＡＰとの認証を行い、この携帯電話機５０とＵＩＭ６０の組み合わせにおいて実行可能なアプリケーションプログラム（本体用ＡＰとこれに対応するモジュール用ＡＰ）を特定する構成である。

【０１４３】このように、ＵＩＭ６０が装着された時点で、この携帯電話機５０とＵＩＭ６０の組み合わせにおいて実行可能なアプリケーションプログラムを特定しておく構成とすれば、個々のアプリケーションプログラムの実行が指示された時に、その都度、本体用ＡＰとこれに対応するモジュール用ＡＰの認証を行う必要がない。したがって、アプリケーションプログラムの実行を指示してから当該アプリケーションプログラムが起動するまでの処理が簡素化され、起動時間を短縮できる。

【０１４４】＜変形例６＞上記第１および第２実施形態では、コンテンツサーバ２０は、インターネット３０に接続されている構成とした。しかしながら、このコンテンツサーバ２０は、移動通信網４０の移動パケット通信網内に設置されている構成であってもよい。また、コンテンツサーバ２０は、専用線を介して移動パケット通信網のゲートウェイサーバに直接接続されている構成であってもよい。さらには、このゲートウェイサーバがコンテンツサーバ２０の機能を有する構成であってもよい。

【０１４５】＜変形例７＞上記第１および第２実施形態では、通信端末として携帯電話機５０、５５を用いた場合について説明した。しかしながら本発明は、例えば、移動通信網４０を介してデータ通信を行うことが可能なＰＤＡやモバイルコンピュータなどに対しても適用可能である。また、ＰＨＳ（Personal Handphone System：登録商標）に対しても適用可能であることは勿論である。また、インターネット３０は、ＬＡＮ（Local Area Network）などのネットワークであってもよい。

【０１４６】＜変形例８＞さらに、図１４に示されるように、通信端末として移動通信網４０を介さず、インターネット３０のみを介してコンテンツサーバ２０とデータ通信を行うことが可能なパーソナルコンピュータ（以下、パソコンと略称する）８０やサーバ９０などに対しても本発明を適用することが可能である。

【０１４７】図１４に示される例は、パソコン８０からサーバ９０にアクセスする場合について示しており、パソコン８０およびサーバ９０の各々は、インターネット３０を介してデータ通信を行う機能を有している。また、コンテンツサーバ２０には、アクセス元のパソコン８０により実行されるパソコン用ＡＰと、アクセス先のサーバ９０により実行されるサーバ用ＡＰとによって構

成されるアプリケーションプログラムが格納されている。

【０１４８】また、パソコン８０は、アクセス先の電子機器（本変形例ではサーバ９０）を特定する情報として、アクセス先となる電子機器の通信アドレス（例えば、ＩＰアドレス）をパソコン用ＡＰと対応付けてメモリに格納する。

【０１４９】本変形例においてパソコン８０およびサーバ９０は、上記第１実施形態において説明したダウンロード処理（図９参照）と同様の処理を実行する。そして、このダウンロード処理においてパソコン８０からの操作入力によって指定されたコンテンツサーバ２０内のパソコン用ＡＰおよびサーバ用ＡＰは、インターネット３０を介してパソコン８０にダウンロードされる。

【０１５０】パソコン８０は、まず、パソコン用ＡＰの送信先となるサーバ９０から当該サーバ９０のシリアルナンバーをインターネット３０経由で取得して、当該シリアルナンバーとダウンロードしたパソコン用ＡＰとを対応付けてメモリに格納する。また、パソコン８０は、サーバ９０の通信アドレスを、このパソコン用ＡＰの処理過程においてアクセスする電子機器の特定情報として、パソコン用ＡＰと対応付けてメモリに格納する。

【０１５１】次いで、パソコン８０は、自機のシリアルナンバーを読み出して、当該シリアルナンバーとダウンロードしたサーバ用ＡＰとをインターネット３０を介してサーバ９０に送信する。サーバ９０では、受信したパソコン８０のシリアルナンバーとサーバ用ＡＰとを対応付けてメモリに格納する。

【０１５２】なお、本変形例においてサーバ用ＡＰは、パソコン８０を経由してサーバ９０にダウンロードされるのではなく、直接、コンテンツサーバ２０からサーバ９０にダウンロードされる形態であってもよい。

【０１５３】そして、パソコン８０およびサーバ９０は、上記第１実施形態において説明したアクセス管理処理（図１０参照）と同様の処理を実行し、プログラムの実行が指示されたパソコン用ＡＰおよびこれに対応するサーバ用ＡＰの相互認証を行う。そして、相互認証されたパソコン用ＡＰおよびサーバ用ＡＰが連携して動作することにより、パソコン８０からサーバ９０に対するアクセスを実現する。

【０１５４】より具体的に説明すると、パソコン８０は、コンテンツサーバ２０からインターネット３０を介して取得したパソコン用ＡＰの実行が指示されると、当該パソコン用ＡＰと対応付けてメモリに格納されている通信アドレスに従って、当該パソコン８０がアクセスするサーバ９０を特定する。

【０１５５】次いで、パソコン８０は、特定したサーバ９０から当該サーバ９０のシリアルナンバーをインターネット３０経由で取得し、パソコン用ＡＰに対応付けられてメモリに格納されているシリアルナンバーと比較す

る。これによりパソコン80は、現時点においてパソコン80とインターネット30を介してデータ通信を行っているサーバ90がこのパソコン用APとペアになるサーバ用APをダウンロードしたサーバ90であるか否かを判断する。

【0156】そして、パソコン80は、当該パソコン80とデータ通信を行っているサーバ90がこのパソコン用APとペアになるサーバ用APをダウンロードしたサーバ90であると判別した場合に、パソコン用APを実行する。このパソコン用APによる処理過程においては、パソコン用APおよびこれに対応するサーバ90内のサーバ用APが連携して動作することにより、パソコン80からインターネット30を介してサーバ90へのアクセスが行われる。

【0157】つまり、パソコン用APの実行時に、パソコン80と通信を行っているサーバ90がパソコン用APとペアになるサーバ用APをダウンロードしたサーバ90と異なる場合や、このサーバ90にパソコン用APに対応するサーバ用APが格納されていなかった場合などは、パソコン用APの実行がキャンセルされ、パソコン80は、サーバ90にアクセスすることができない。

【0158】このように、インターネット30を介して取得したパソコン用APの実行については、パソコン80とサーバ90との間で上述した一定の条件が成立した場合のみ実行が許可され、これによりパソコン80からサーバ90へのアクセスが可能となる。なお、アクセス対象は、サーバ90に格納されている個人情報に限定されず、サーバ90内のその他の格納データであってもよい。さらに、パソコン80からサーバ90へのアクセスは、データ以外の、例えば、サーバ90に格納されているプログラムの起動であってもよい。また、サーバ90内の入出力ポートへのアクセスなどであってもよい。

【0159】したがって、パソコン80は、インターネット30を介して取得したプログラムの実行に際し、セキュリティを確保しつつ、このプログラムに従って当該パソコン80外のリソース、すなわち、当該パソコン80とインターネット30を介してデータ通信を行うことが可能な電子機器に格納されているデータへのアクセスやプログラムの起動、入出力ポートへのアクセスなどを行うことができる。

【0160】なお、本実施形態において、アクセス元のパソコン80やアクセス先のサーバ90は、インターネット30を介して他のコンピュータとデータ通信を行うことが可能な通信装置であればよく、パソコンやサーバに限定されるものではない。

【0161】＜変形例9＞上記第1および第2実施形態では、オープンネットワークを介して組み込まれるプログラムが、JavaアプレットやJavaアプリケーションなどのJavaプログラミング言語で記述されたプログラムであ

る場合について説明した。しかしながら、本発明において、Java以外のプログラミング言語で記述されたプログラムを本体用APやモジュール用AP、電子機器用APとして用いてもよいことは勿論である。

【0162】例えば、図15に示された本体用APとモジュール用APの実行環境を示す機能階層モデルにおいて、本体用AP「α」は、携帯電話機50用のOS上で実行されるアプリケーションプログラムであって、JAMおよびJavaVMを介せずにCPU506が実行可能である。また、この本体用AP「α」に対応するモジュール用AP「α」は、UIM60用のOS上で実行されるアプリケーションプログラムであって、Java Card VMを介せずにCPU604が実行可能である。このように、共にOS上で実行される本体用AP「α」およびモジュール用AP「α」に対して本発明を適用することも可能である。

【0163】＜変形例10＞上記第1および第2実施形態において、UIM60は、携帯電話機50、55などの通信端末と無線通信などによりデータの送受信を行う非接触型のICカードであってもよい。この場合、携帯電話機50、55のUIMインタフェース505は、当該携帯電話機50、55に装着されたUIM60との間で無線通信によって行われるデータの送受信を制御する。

【0164】

【発明の効果】以上説明したように本発明によれば、通信端末は、セキュリティを確保しつつ、ネットワークを介して得たプログラムに従って当該プログラムのダウンロード元を除く当該通信端末外のリソースにアクセスすることができる。

【図面の簡単な説明】

【図1】 この発明の第1実施形態に係るコンテンツサーバ、携帯電話およびUIMを含む移動通信システムの構成を示すブロック図である。

【図2】 同実施形態に係るコンテンツサーバのハードウェア構成を示すブロック図である。

【図3】 同実施形態に係るコンテンツサーバのAP格納領域の構成を示す図である。

【図4】 同実施形態に係る携帯電話機のハードウェア構成を示すブロック図である。

【図5】 同実施形態に係る携帯電話機において、不揮発性メモリのAP格納領域の構成を示す図である。

【図6】 同実施形態に係るUIMのハードウェア構成を示すブロック図である。

【図7】 同実施形態に係るUIMにおいて、EEPROMのAP格納領域の構成を示す図である。

【図8】 同実施形態に係る本体用APとモジュール用APの実行環境を示す模式図である。

【図9】 同実施形態に係るコンテンツサーバからアプリケーションプログラムをダウンロードする場合の、コ

ンテンツサーバ、携帯電話機およびUIMの動作を例示するシーケンスチャートである。

【図10】 同実施形態に係る携帯電話機がUIM内の加入者情報にアクセスする場合の、携帯電話機およびUIMの動作を例示するシーケンスチャートである。

【図11】 本発明の第2実施形態に係る携帯電話機のハードウェア構成を例示するブロック図である。

【図12】 変形例1において、コンテンツサーバからアプリケーションプログラムをダウンロードする場合の、コンテンツサーバ、携帯電話機およびUIMの動作を例示するシーケンスチャートである。

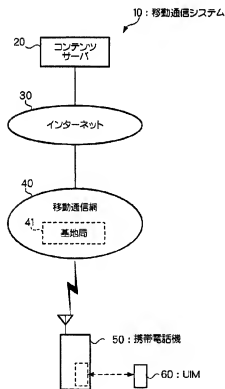
【図13】 変形例4に係るアクセス規定データのデータ構成を例示する図である。

【図14】 変形例8に係るコンテンツサーバ、パソコンおよびサーバを含む通信システムの構成を例示するブロック図である。

【図15】 変形例9に係る本体用APとモジュール用APの実行環境を例示する模式図である。

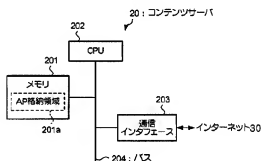
【符号の簡単な説明】

【図1】

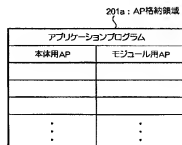


10……移動通信システム、20……コンテンツサーバ、30……インターネット、40……移動通信網、50、55……携帯電話機、60……UIM、70……電子機器、80……パソコン、90……サーバ、201……メモリ、201a……AP格納領域(アプリケーションプログラム格納領域)、202……CPU、203……通信インタフェース、204……バス、501……無線通信部、501a……アンテナ、502……操作部、503……通話処理部、504……表示部、505……UIMインタフェース、506……CPU、507……記憶部、508……ROM、509……RAM、510……不揮発性メモリ、510a……シリアルナンバー格納領域、510b……AP格納領域、511……バス、550……赤外線通信部、601……外部インタフェース、602……ROM、603……RAM、604……CPU、605……EEPROM、605a……シリアルナンバー格納領域、605b……AP格納領域、605c……加入者情報格納領域、606……バス。

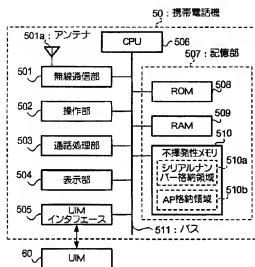
【図2】



【図3】



【図4】



【図5】

510b: AP格納領域

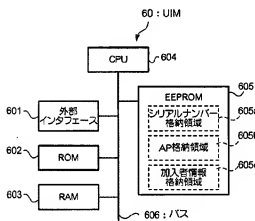
シリアルNo. (UIM)	本体用AP

【図7】

605b: AP格納領域

シリアルNo.(本体)	モジュール用AP

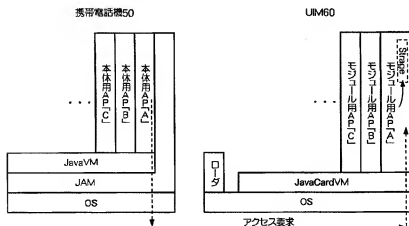
【図6】



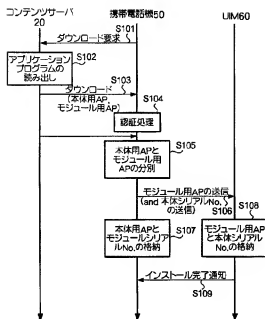
【図13】

識別情報	アクセス行為	可否
本体用AP「A」	読み出し	1
	書き換え	1
	追加	1
	削除	0

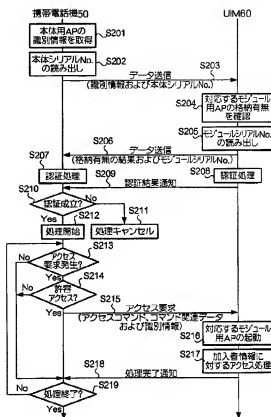
【図8】



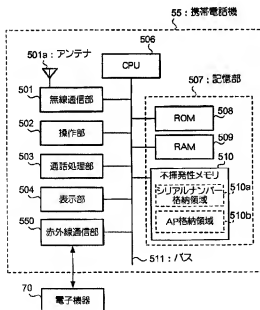
【図9】



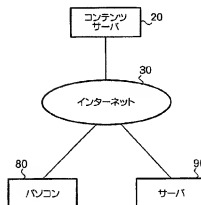
【図10】



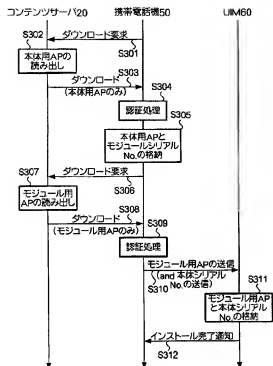
【図11】



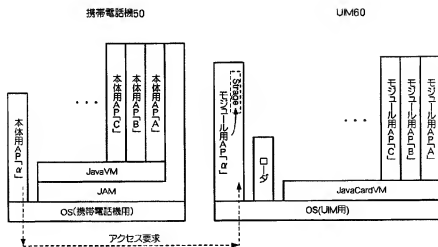
【図14】



【図12】



【図15】



フロントページの続き

(51) Int. Cl.⁷
 G 0 6 F 15/00
 H 0 4 M 1/00
 3/487

識別記号

F I
 H 0 4 M 1/00
 3/487
 G 0 6 F 9/06

キーワード(参考)
 V 5 K 0 2 7

6 6 0 G

- (72)発明者 東 明洋
東京都千代田区永田町二丁目11番1号 株
式会社エヌ・ティ・ティ・ドコモ内
- (72)発明者 野田 千恵
東京都千代田区永田町二丁目11番1号 株
式会社エヌ・ティ・ティ・ドコモ内
- (72)発明者 古瀬 正浩
東京都千代田区永田町二丁目11番1号 株
式会社エヌ・ティ・ティ・ドコモ内
- (72)発明者 上田 誠
東京都千代田区永田町二丁目11番1号 株
式会社エヌ・ティ・ティ・ドコモ内

- (72)発明者 若林 達明
東京都千代田区永田町二丁目11番1号 株
式会社エヌ・ティ・ティ・ドコモ内
- (72)発明者 平松 孝朗
東京都千代田区永田町二丁目11番1号 株
式会社エヌ・ティ・ティ・ドコモ内
- F ターム(参考) 5B017 AA06 BA09 BB09 BB10 CA15
5B076 BB06 FB02
5B085 AE04 AE12
5K015 AF02 GA01
5K024 AA71 CC11 FF01
5K027 AA11 BB01 CC08 HH26 MM03